



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10162067 A**(43) Date of publication of application: **19.06.98**

(51) Int. Cl. **G06F 17/60**  
**G06K 17/00**

(21) Application number: **08317828**(71) Applicant: **U CARD:KK**(22) Date of filing: **28.11.96**(72) Inventor: **OCHIAI YUJI**

(54) **INFORMATION REGISTERING METHOD  
 UTILIZING NETWORK**

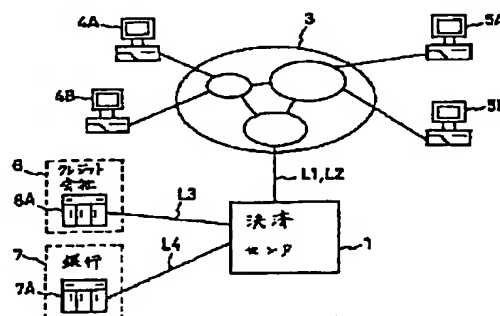
together with history information on the individual and saved in a file.

## (57) Abstract:

COPYRIGHT: (C)1998,JPO

**PROBLEM TO BE SOLVED:** To make the security of held information high by making a terminal transmit a telegraphic message consisting of information and a verification key signing with a signature key generated in a pair with the verification key to a center through a network for registration, and also decodes the signature key and holds it.

**SOLUTION:** This method is constituted of a settlement center 1, the network 3, general member terminals 4A and 4B, member store terminals 5A and 5B, a center device 6A of a credit company 6, and a center device 7A of a bank 7. A 1st password and a 2nd password for ciphering are inputted and registration contents to the settlement center 1 are inputted. Then, the signature key and a 'kind' for generating the verification key paired with the signature key so as to verify the signature key are inputted. The signature key and verification key corresponding to the inputted 'kind' are generated. The signature key is ciphered with the 2nd password and further ciphered with the 1st password



(51) Int.Cl.<sup>8</sup>

識別記号

F I

G 0 6 F 17/60

G 0 6 F 15/21

3 4 0 Z

G 0 6 K 17/00

G 0 6 K 17/00

T

G 0 6 F 15/21

3 3 0

審査請求 未請求 請求項の数 4 O L (全 9 頁)

(21) 出願番号

特願平8-317828

(22) 出願日

平成8年(1996)11月28日

(71) 出願人 393007868

株式会社ユーカード

東京都渋谷区元代々木町30-13

(72) 発明者 落合 祐二

東京都渋谷区元代々木町30-13 日交元

代々木ビル 株式会社ユーカード内

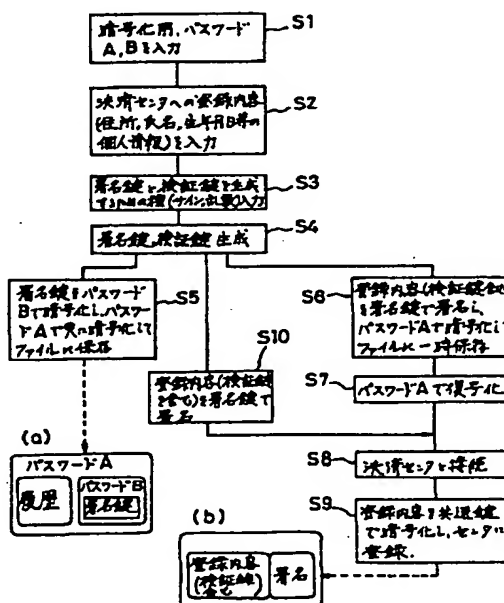
(74) 代理人 弁理士 山川 政樹

(54) 【発明の名称】 ネットワークを利用した情報の登録方法

(57) 【要約】

【課題】 ネットワークを介して個人情報などの情報を登録する場合及び登録した情報について高セキュリティを確保する。

【解決手段】 各端末4、5の利用者は決済センタ1への会員登録時には自身の個人情報と検証鍵とに署名鍵で署名を行ったうえ共通鍵で暗号化して決済センタ1へ送信し、かつ検証鍵と対の上記署名鍵をパスワードBで暗号化したうえ、パスワードAでさらに暗号化し自身の端末のファイルに保管する。ここで商品の取引及び決済時等には決済センタへ送信する電文に対し署名鍵により署名を行う一方、決済センタは、電文を受信すると登録してある検証鍵により署名の確認を行う。この結果、商品の決済時等に高セキュリティを確保でき、また他人にパスワードAが解読されても署名鍵はパスワードBで更に暗号化されているため署名鍵は本人のみの使用に限定され、電子署名による証拠取引等を行う際に高セキュリティを確保できる。



## 【特許請求の範囲】

【請求項1】 ネットワークを介してセンタと端末とが接続され、端末の情報をネットワークを介して電文としてセンタへ送信し登録するネットワークを利用した情報の登録方法であって、

前記端末は前記情報とこの情報の検証を行うための第1の鍵とからなる前記電文に対し、前記第1の鍵と対に生成される第2の鍵により署名を行ってネットワークを介してセンタへ送信し登録させると共に、前記第2の鍵をパスワードで暗号化して保持することを特徴とするネットワークを利用した情報の登録方法。

【請求項2】 請求項1において、前記パスワードは第1及び第2のパスワードからなり、前記端末は前記第1のパスワードで前記第2の鍵を暗号化すると共に、第1のパスワードで暗号化された第2の鍵を第2のパスワードで暗号化して保持することを特徴とするネットワークを利用した情報の登録方法。

【請求項3】 請求項2において、前記端末は、センタに署名電文を送信する場合は第1のパスワードで暗号化して一時保存すると共に、センタへの送信時にこの署名電文を第1のパスワードで復号化し、かつセンタとの間で一時的に生成される第3の鍵により暗号化して送信し、センタではこの署名電文を受信すると第3の鍵により復号化して登録することを特徴とするネットワークを利用した情報の登録方法。

【請求項4】 請求項1ないし請求項4の何れかの請求項において、前記情報の登録後に、前記端末から第2の鍵により署名された電文が送信された場合、センタは登録された第1の鍵によりこの署名電文を検証することを特徴とするネットワークを利用した情報の登録方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、ネットワークを介して個人情報などの情報を登録する際の情報の登録方法に関する。

## 【0002】

【従来の技術】 マルチメディア技術の進歩やインターネットの普及により、電子商取引（エレクトロニック・コマース）が現実化しつつある。このようなネットワーク上の決済手段の1つとして、クレジットカードによる決済手段が知られている。

## 【0003】

【発明が解決しようとする課題】 このような決済システムでは、ネットワークを介して個人情報をセンタに登録しておく必要がある。しかし、こうした決済システムは、インターネット等のネットワークを介在して不特定多数間で電子商取引が行われるため、他人に勝手に個人情報を利用されて不正な取引が行われる恐れがあり、従って暗号技術や本人認証等のセキュリティに関して万全

の体制をとることが要望されている。従って本発明は、ネットワークを介して個人情報などの情報を登録する場合及び個人情報を保持する場合に高セキュリティを確保することを目的とする。

## 【0004】

【課題を解決するための手段】 このような課題を解決するために本発明は、ネットワークを介してセンタと端末とが接続され、端末の情報をネットワークを介して電文としてセンタへ送信して登録する場合、端末は、上記情報とこの情報の検証を行うための第1の鍵（検証鍵）とからなる上記電文に対し、検証鍵と対に生成される第2の鍵（署名鍵）により署名を行ってネットワークを介してセンタへ送信し登録させると共に、端末では署名鍵をパスワードで暗号化して保持するようにした方法である。従って、端末側から個人情報などの情報を電文としてセンタに送信し登録する場合、端末側で個人情報に個人の署名を行ってセンタへ送信すると共に、この署名鍵をパスワードで暗号化して保管するようにしたので、ネットワークを介して登録される個人情報の高セキュリティ性を確保でき、従ってこうした個人情報の第三者による不正使用を的確に防止できる。また、パスワードは個人のみで管理されるため、パスワードの不正使用は本人の不注意によるリークなどによって本人が関与した場合に限られ、システム全体として高いセキュリティを保つことができる。また、上記パスワードを第1及び第2のパスワードから構成し、端末は第1のパスワード（パスワードB）で署名鍵を暗号化すると共に、第1のパスワードで暗号化された署名鍵をさらに第2のパスワード（パスワードA）で暗号化して保持するようにした方法である。従って、第三者に第1のパスワードが解読されたとしても、署名鍵は第2のパスワードでさらに暗号化されているため署名鍵は本人のみの使用に限定され、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。また、端末は、センタへ署名電文を送信する場合は第1のパスワードで暗号化して一時保存すると共に、センタへの送信時点でこの署名電文を第1のパスワードで復号化した後、センタとの間で一時的に生成される共通鍵（第3の鍵）により暗号化して送信し、センタではこの署名電文を共通鍵で復号化したのち登録するようにした方法である。従って、センタに個人情報を登録する場合、より高いセキュリティ性を確保できる。また、上記情報の登録後に、端末から署名鍵により署名された電文が送信された場合、センタは登録された検証鍵によりこの署名電文を検証するようにした方法である。従って、センタでは登録されている検証鍵によりこの電文が真に署名されているか否かを確認でき、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。

## 【0005】

【発明の実施の形態】 以下、本発明について図面を参照

して説明する。図1は本発明を適用したシステムの構成を示すブロック図である。同図において、1は決済センタ、3はインターネット等のネットワーク、4A、4Bは一般会員の所有する端末（以下、一般会員端末）、5A、5Bは店舗会員の所有する端末（以下、店舗会員端末）、6Aはクレジット会社6のセンタ装置、7Aは銀行7のセンタ装置である。

【0006】即ち、一般会員端末4A、4Bはネットワーク3を介して店舗会員端末5A、5Bに接続されていると共に、決済センタ1は専用回線L1またはL2を介してネットワーク3に接続されている。また、決済センタ1はDDX回線L3を介してクレジット会社のセンタ装置6Aに接続され、また専用回線L4を介して銀行のセンタ装置7Aに接続されている。

【0007】ところで、売り手である店舗会員端末5に陳列される商品としては、既存の通信販売形態によって販売される商品（後日配送商品）、その場で販売される文書、ソフトウェア、画像等の商品、及びリアルタイムでコンピュータを運用するゲーム等の商品がある。一方、買い手である一般会員は、例えば決済センタ1の銀行口座等に予め所定額を振り込み、これが決済センタ1により確認されることにより決済センタ1から発行された所定額の価値情報が付与された仮想プリペイドカードを取得している。ここで、店舗会員端末5からネットワーク3を介して提供され端末4に表示される商品が一般会員によって購入されると、決済センタ1ではその一般会員に付与した仮想プリペイドカードの価値情報から購入商品の価格を減じると共に、該店舗会員に対してその購入商品の対価の支払を行う。

【0008】次に図2は、決済センタ1の構成を示すブロック図である。同図において、12はルーター11により選択された回線を介しネットワーク3との間で各種の情報を授受するWWWサーバ、13はネットワーク3からの決済センタ1に対する不正なアクセスを防ぐ働きをするセキュリティサーバ、14はクレジット会社6または銀行7とデータ通信を行う通信サーバ、15は送信電文（送信データ）の作成、受信電文（受信データ）の解析及びこれらの電文に対し後述の電子署名や署名検証等を行う通信処理サーバ、16はこれらの処理情報を蓄積するデータベース、17は決済センタ1においてデータ処理時に発生したエラー情報の出力やログ情報を出力するプリンタである。

【0009】また、18は決済サーバであり、決済サーバ18は、加入者原簿（一般会員原簿）、店舗原簿、上記暗号化や電子署名の際に必要な署名鍵及び検証鍵等の原簿及び処理番号原簿等のデータベース19に対する記憶管理を行うと共に、通信サーバ15からの受信データを入力するとデータベース19の記憶内容に基づき各一般会員に発行した仮想プリペイドカードの決済処理を行い、その処理結果を送信データとして通信処理サ

ーバ15に与えるものである。また、20は検索・照会処理、会員の登録処理、返金処理及び統計資料作成処理等を行ってプリンタ21に出力する照会・統計用サーバである。なお、23は以上の各部で処理された情報をバックアップするバックアップセンタである。

【0010】次に図3以降の各図面を用い、本システムの各部の処理動作を具体的に順を追って説明する。まず本システムへの会員の加入処理から説明する。図3は本システムに対する一般会員の加入処理を示す図である。

10 決済センタ1では、ネットワーク3上に常時、一般会員加入申込用の案内画面を送信している（時点①）。ここで、その案内画面を入力したネットワーク3の利用者が端末4から加入要求を行うと（時点②）、決済センタ1では加入画面を作成して端末4へ送る（時点③）。この加入画面を入力した上記利用者が端末4から加入申込を行うと（時点④）、決済センタ1では暗号関数等を用いた入会承認用アプリケーションソフト（以下、APソフト）が準備してあり、利用者がそのAPソフトを端末4へダウンロードする（時点⑤）。その後、決済センタ1  
20 では、上記利用者である加入申込者宛に一般会員番号利用規約等を郵送し（時点⑥）、加入申込者がこれを確認して端末4からAPソフトを使用し、暗号を用いた会員登録データを送信する（時点⑦）と、決済センタ1ではデータベース19に会員原簿として登録する。このようにして商品の買い手である一般会員の加入が行われる。

【0011】次に店舗会員の加入は図4に示す手順で行われる。即ち、決済センタ1からネットワーク3上に送信される店舗会員加盟申込用の案内画面（時点①）に対し、その案内画面を入力したネットワーク3の利用者が端末5から加入要求を行うと（時点②）、決済センタ1では加入画面を作成して端末5へ送る（時点③）。この加入画面を入力した上記利用者が端末5から加入申込を行うと（時点④）、決済センタ1では暗号関数等を用いた加盟承認用APソフトが準備してあり、利用者がそのAPソフトを端末5へダウンロードする（時点⑤）。その後、決済センタ1では、上記利用者である加盟申込者宛に店舗会員番号加盟店約款等を郵送し（時点⑥）、加盟申込者がこれを確認して端末5からAPソフトを使用し暗号を用いた店舗登録データを送信する（時点⑦）  
40 と、決済センタ1ではデータベース19に店舗会員原簿として登録する。このようにして商品の売り手である店舗会員の加盟が行われる。

【0012】こうして各会員が本システムに加入した後、一般会員は、図5に示すように、端末4からネットワーク3を介し後述の電子署名や暗号等を用いた仮想プリペイドカード要求データを決済センタ1へ送信する（時点①）。すると、決済センタ1ではその一般会員からの入金を確認し、電子署名や暗号等を用いた所定額の価値情報の仮想プリペイドカードをその一般会員宛に発行する（時点②）。一般会員は時点②でその仮想プリペ

イドカードをネットワーク3を介して取得する。

【0013】図12～図15は決済センタ1によるこのような仮想プリペイドカードの発行例を示す図である。即ち、図12の例では、まず一般会員が端末4を用いてプリペイド要求を行う（時点①）。すると決済センタ1ではクレジット会社6に対しこの一般会員に関する与信情報を問い合わせ、与信情報が得られると（時点②）、その一般会員に対して所定額の価値情報を付与した仮想プリペイドカードを発行することで、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点③）。その後、決済センタ1ではクレジット会社6からその所定額を入金し（時点④）、クレジット会社6では、銀行7の上記一般会員の口座から所定額を引き落とす（時点⑤）。

【0014】次に、図13の例では、まず一般会員が端末4を用いてプリペイド要求を行う（時点①）と共に、回線を介して自身の口座を有する銀行71または郵便局81に対し、決済センタ1と取引のある銀行72または郵便局82への所定額の振り込みを指示する（時点②）。すると、銀行71または郵便局81により、決済センタ1と取引のある銀行72または郵便局82へ所定額の振り込みが行われる（時点③）。決済センタ1では銀行72または郵便局82にプリペイド要求を行った上記会員からの入金を確認し、入金が確認されると（時点④）、上記会員宛に所定額の仮想プリペイドカードを発行する。この結果、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点⑤）。

【0015】次に、図14の例では、まず一般会員が端末4を用いてプリペイド要求を行う（時点①）と共に、決済センタ1と取引のある銀行7または郵便局8への所定額の振り込みを行う（時点②）。すると、決済センタ1では銀行7または郵便局8にプリペイド要求を行った上記会員からの入金を確認し、入金が確認されると（時点③）、上記会員宛に所定額の仮想プリペイドカードを発行する。この結果、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点④）。

【0016】次に、図15の例では、まず一般会員が端末4を用いてプリペイド要求を行う（時点①）と共に、決済センタ1宛に現金書留を郵送する（時点②）。すると、決済センタ1ではプリペイド要求を行った上記会員からの現金書留を受領し入金が確認されると（時点③）、上記会員宛に所定額の仮想プリペイドカードを発行する。この結果、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点④）。

【0017】こうして一般会員は価値情報が付与された仮想プリペイドカードを取得すると、図6に示すように、端末4を操作し、店舗会員端末5からネットワーク3を介して提供され端末4に表示される各商品のうち、購入したい何れかの商品を選択し（時点①）、受発注処理を完了させて（時点②）、その代金精算を決済センタ

1へ指示する（時点③）。すると、一般会員端末4と店舗会員端末5との間で以下に示すような取引処理が開始される。

【0018】即ち、図7に示すように、この場合まず端末4から電子署名および暗号が施された取引番号等の要求情報（支払指示）がネットワーク3を介して決済センタ1へ送られる（時点①）。すると、決済センタ1では

この取引番号要求を行った会員が一般会員であることを確認のうえ、その一般会員の残高認証を行い（時点②）、ネットワーク3を介して端末5に対し電子署名および暗号を施した取引番号等の要求情報（支払通知）を送信する（時点③）と共に、端末4に対して新残高を通知する（時点④）。この結果、一般会員及び店舗会員の決済が完了する。

【0019】このようにして商品の売買及び決済処理が行われた後、店舗会員端末5からネットワーク3を介して一般会員端末4宛に販売商品の受け渡しが行われる

（図8）。なお、ここでネットワーク3を介して配送される商品の類としては、上述した文書、ソフトウェア及び画像等の商品があり、既存の通信販売形態の商品は、後日配送される。そして販売商品の配送が行われた後、図9に示すように、店舗会員端末5から決済センタ1に対してその販売商品に相当する代金の支払請求が送信される（時点①）。すると、決済センタ1では、銀行7の該店舗会員の口座に該代金相当額を振り込む（時点②）。

【0020】このように本システムは、商品の買い手はクレジットカードまたはホームバンキングの手段で決済センタ1から仮想プリペイドカードを購入し、電子商取引を行う一方、商品の売り手は電子商取引にあたって決済センタ1を介し買い手の仮想残高を商品代金分だけ減額すると共に、決済センタ1に対して代金請求を行い支払を受けるようにしたものである。

【0021】図10は、本発明の要部動作を示すもので、各端末4、5から決済センタ1に対し会員登録を行う場合の各端末4、5の動作状況を示す流れ図であり、図10に示すような各ステップを踏むことによりシステムとして高いセキュリティ性を確保できる。即ち、ステップS1では、まず2つの暗号化用パスワードA（第1のパスワード、及びパスワードB（第2のパスワード））を入力する。続いてステップS2では、決済センタ1への登録内容の入力操作を行う。この登録内容としては、会員個人の住所、氏名、生年月日等の個人情報が含まれる。そして続いてステップS3では後述の署名鍵（秘密鍵；印鑑に相当）及びこの署名鍵を検証する為の署名鍵と対になる検証鍵（公開鍵）を生成するための「種」を入力する。ここでこの「種」を入力する場合は、例えば会員個人の自筆によるサインが端末4の図示しないキーボードから入力されるか、或いは、端末4内で乱数を用いて自動的に入力される。すると、ステップS4では入

10

20

30

40

50

力された「種」に応じた署名鍵及び検証鍵が生成される。ここで、署名鍵及び検証鍵を生成する場合は、署名鍵の関数が検証鍵となるように生成される。即ち、一例として署名鍵を  $p$ 、 $q$  とした場合、検証鍵  $n$  は、 $n = p^2 \times q$  となるように生成される。

【0022】生成された署名鍵は各端末4、5においてそれぞれ図示しないファイルに保存される。ここで署名鍵をファイルに保存する場合は、ステップS5で署名鍵をパスワードBで暗号化し、これをさらにパスワードAにより、その個人の履歴情報（即ち、この場合は個人の商品購入履歴情報）とともに暗号化してファイルに保存する。この結果、署名鍵は図10（a）に示すような階層構造でファイルに保管される。従って、第三者にパスワードAが解読されたとしても、第三者はそのパスワードAに該当する個人の商品購入履歴情報等を端末の図示しない表示部に表示できるのみであり、署名鍵はパスワードBでさらに暗号化されているために第三者による商品購入等の決済を伴う行為（署名が必要なサービス）に使用されることはなく、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。

【0023】次に決済センタ1に対して上述の入力内容を登録する場合は、次のような2通りの方法がある。まず、第1の方法は、ステップS2で入力した内容とステップS4で生成された検証鍵に対しステップS6で署名鍵により署名し、これをパスワードAにより暗号化してファイルに一旦保存する。次いでステップS7でパスワードAによる暗号を解いた（復号化）後、ステップS8で決済センタ1と回線接続を行う。そしてその後、ステップS9でその登録内容を決済センタ1との伝送の際に一時的に生成される共通鍵（暗号鍵）により暗号化し、決済センタ1へ伝送する。決済センタ1ではこの電文を上記共通鍵により復号化して登録する。次に第2の方法は、ステップS2で入力した内容とステップS4で生成された検証鍵に対しステップS10で署名鍵により署名したのち、ステップS8で決済センタ1と回線接続を行う。そしてその後、ステップS9でその登録内容を決済センタ1との伝送の際に一時的に生成される共通鍵（暗号鍵）により暗号化し、決済センタ1へ伝送する。決済センタ1ではこの電文を上記共通鍵により復号化して登録する。

【0024】このようにして一般会員や店舗会員の個人データが図10（b）に示すような形態で決済センタ1に登録される。その後、決済センタ1では各端末から署名鍵により署名された電文が送られてきた場合、後述するようにその署名鍵と対の検証鍵により、その電文が真に電子署名されているか否かを検証するため、商品取引において信頼性の高いシステムを実現できる。

【0025】図11は、こうして決済センタ1に登録された一般会員の端末4が電子商取引を行う場合の動作を示す流れ図である。即ち、決済センタ1と未接続状態

（オフライン状態）にある一般会員端末4においてステップS11でパスワードAの入力操作が行われると、その一般会員端末4に保存された過去の取引データ（即ち、買い物履歴データ；商品購入履歴情報）をステップS12で図11（a）に示す表示データとして端末4の図示しない表示部に表示させる。なお、図11（a）において、 $yy$ 、 $mm$ 、 $dd$ は各々、年、月、日を示す。

【0026】続いて上記一般会員端末4においてステップS13でパスワードBの入力操作が行われると、この会員端末4では、決済センタ1に送信される電文（即ち、例えば図7の説明で述べた取引番号要求データ）に署名を行うための署名鍵が取り出されたものと判断し、ステップS14において決済センタ1との間で署名が必要なサービスへ移行する。即ち、上述のパスワードBの入力により署名鍵が取り出され決済センタ1と回線接続が行われた後、上記の電文がその署名鍵で署名されこの署名電文がその一般会員端末4から送信されたとすると、決済センタ1ではこの電文を受信し、会員登録時に登録されている検証鍵によりこの受信電文を解読し確認する。そして確認がOKになると、その一般会員の残高認証を行った後に店舗会員端末5に対し電子署名および暗号を施した支払通知を送信すると共に、その一般会員端末4に対し新残高を通知する。

【0027】このように、決済時には必ず使用される署名鍵をパスワードA、Bにより暗号化するため、パスワードAが解読され署名鍵の在処が第三者に分かってしまったような場合でも、第三者は署名鍵を取り出すことができず、従って第三者による署名鍵の使用を防止することができる。即ち、この場合、第三者はこの署名鍵の持ち主の例えば買い物履歴等が閲覧できるだけであって、署名が必要な決済サービスへの移行を阻止できる。また、第三者が署名鍵を偶然入手したとしても、署名鍵を利用し難いという効果も期待でき、またパスワードBを偶然入手したとしてもパスワードAを入手しない限り署名鍵を取り出せないことから、パスワードBの利用を阻止する効果も期待できる。

【0028】さらに、署名鍵と検証鍵とを対に設け、署名鍵は各端末で管理し、検証鍵は決済センタ1で一括して管理することにより、署名鍵が第三者の手に渡ってしまった場合でも決済が必要な商取引時には第三者は必ず決済センタ1を利用して検証鍵により電文を解読させなければならないため、署名鍵の暗号化の度合いを弱めることもできる。従って、署名鍵を暗号化する場合パスワードAのみで行い、パスワードBを不要にすることができる。

【0029】

【発明の効果】以上説明したように本発明によれば、ネットワークを介してセンタと端末とが接続され、端末側から個人情報などの情報を電文としてセンタに送信し登録する場合、端末側で個人情報に個人の署名を行ってセ

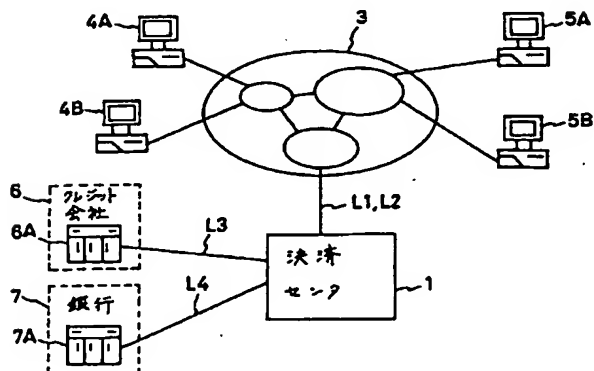


ンタへ送信すると共に、この署名鍵をパスワードで暗号化して保管するようにしたので、ネットワークを介して登録される個人情報の高セキュリティ性を確保でき、従ってこうした個人情報の第三者による不正使用を的確に防止できる。また、パスワードは個人のみで管理されるため、パスワードの不正使用は本人の不注意によるリークなどによって本人が関与した場合に限られ、システム全体として高いセキュリティを保つことができる。また、上記パスワードを第1及び第2のパスワードから構成し、端末は第1のパスワードで署名鍵を暗号化すると共に、第1のパスワードで暗号化された署名鍵をさらに第2のパスワードで暗号化して保持するようにしたので、第三者に第1のパスワードが解読されたとしても、署名鍵は第2のパスワードでさらに暗号化されているため署名鍵は本人のみの使用に限定され、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。また、端末は、センタに署名電文を送信する場合は第1のパスワードで暗号化して一時保存すると共に、センタへの送信時点でこの署名電文を第1のパスワードで復号化した後、共通鍵で暗号化して送信し、センタではこの署名電文を共通鍵で復号化して登録するようにしたので、センタに個人情報を登録する場合、より高いセキュリティ性を確保できる。また、上記個人情報の登録後に、端末から署名鍵により署名された電文が送信された場合、センタは登録された検証鍵によりこの署名電文を検証するようにしたので、センタではこの電文が真に署名されているか否かを確認でき、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。

#### 【図面の簡単な説明】

【図1】 本発明のシステムの構成を示すブロック図である。

【図1】



【図2】 上記システムを構成する決済センタのブロック図である。

【図3】 一般会員の登録動作を示す図である。

【図4】 店舗会員の登録動作を示す図である。

【図5】 一般会員端末を介する仮想プリペイドカード取得動作を示す図である。

【図6】 一般会員端末を介する購入商品の選択動作及び受発注動作を示す図である。

【図7】 商品取引時の決済動作を示す図である。

【図8】 商品取引時の商品引き渡し状況を示す図である。

【図9】 商品取引時の決済センタの支払動作を示す図である。

【図10】 各端末が決済センタに対し会員登録を行う場合の動作状況を示す流れ図である。

【図11】 一般会員端末が電子商取引を行う場合の動作を示す流れ図である。

【図12】 仮想プリペイドカード取得の第1の例を示す図である。

【図13】 仮想プリペイドカード取得の第2の例を示す図である。

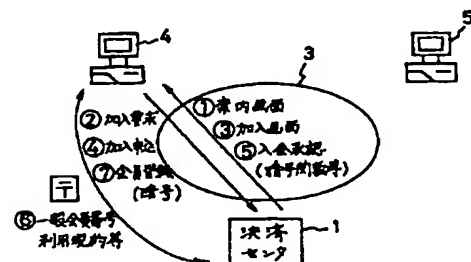
【図14】 仮想プリペイドカード取得の第3の例を示す図である。

【図15】 仮想プリペイドカード取得の第4の例を示す図である。

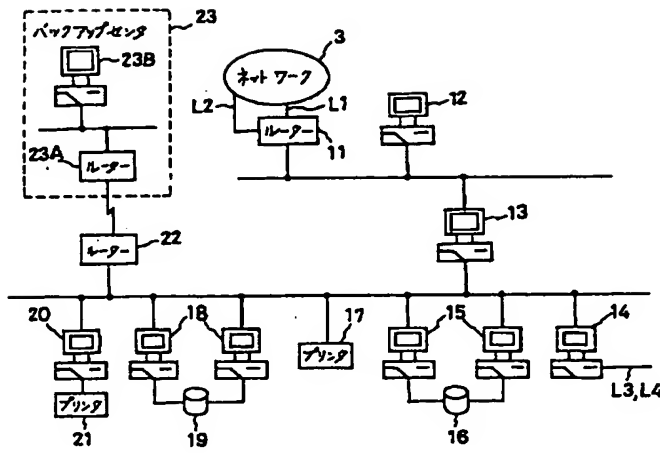
#### 【符号の説明】

1…決済センタ、3…ネットワーク、4、4A、4B…一般会員端末、5、5A、5B…店舗会員端末、6…クレジット会社、7、71、72…銀行、8、81、82…郵便局、6A、7A、8A…センタ装置、11、22…ルーター、12～15、17、18、20…サーバー、23…バックアップセンタ。

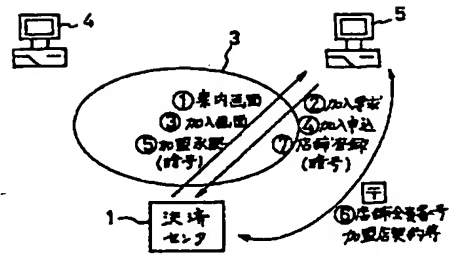
【図3】



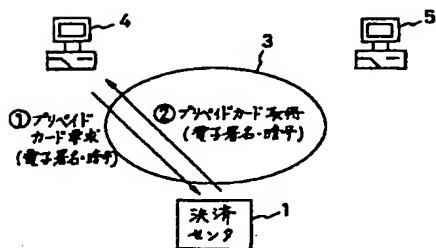
【図2】



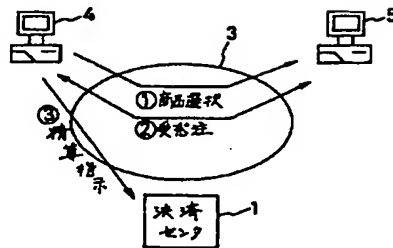
【図4】



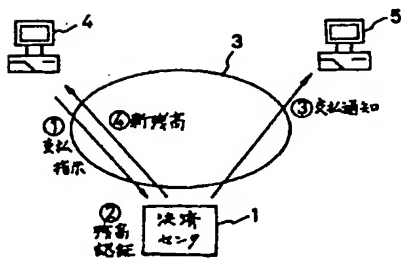
【図5】



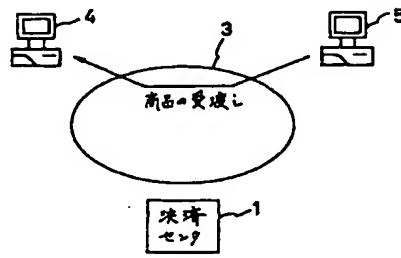
【図6】



【図7】



【図8】







【図10】

